Aufstellung für Auftraggeber der opta data Finance GmbH

zu den bei der opta data Finance GmbH getroffenen technischen und organisatorischen Maßnahmen im Datenschutz.

Vorwort

Die familiengeführte opta data Gruppe entwickelt seit über 50 Jahren passgenaue Services und digitale Lösungen für den betrieblichen Alltag in verschiedensten Bereichen des Gesundheitswesens – mit dem Ziel, die nahezu 60.000 Kund:innen bestmöglich zu unterstützen. Über 2.500 engagierte Mitarbeiter:innen bieten darüber hinaus bankenunabhängige Finanzierungen, digitale Kommunikationsprodukte oder gezieltes Telefonmarketing.

Als Innovationsführer gestalten wir die Digitalisierung des Gesundheitswesens aktiv mit und sind Marktführer auf dem Gebiet der Telematikinfrastruktur.

Wir legen großen Wert auf die Zufriedenheit unserer Kund:innen und die Gesundheit unserer Kolleg:innen. Ein Einsatz, für den wir mehrfach ausgezeichnet wurden: mit den Siegeln „Top Job", „Deutschlands Kundenchampions" und dem „Corporate Health Award" für unser Engagement im betrieblichen Gesundheitsmanagement.

Diese Auflistung der bei der opta data Finance GmbH getroffenen technischen und organisatorischen Maßnahmen im Datenschutz (TOMs) orientiert sich an den Vorgaben des § 64 BDSG, der für nicht öffentliche Stellen keine Gültigkeit hat, gleichzeitig aber eine strukturierte Dokumentation der TOMs ermöglicht, da es weder in der EU-Datenschutzgrundverordnung (DSGVO) noch im neuen Bundesdatenschutzgesetz (BDSG) dazu Vorgaben für nicht öffentliche Stellen gibt. Diese Angaben dokumentieren auch die Forderungen des § 26 KDG und des Art. 32 der DSGVO. Es soll Verantwortlichen (Auftraggebern) dazu dienen, ihre Prüf- und Dokumentationspflicht bei Auftragsverarbeitung gem. Artt. 28, 29 DSGVO, § 29 KDG und § 80 SGB X zu erleichtern.

Diese Aufstellung ist auch als Ergänzung zu einem bestehenden oder neuen, Art. 28, 29 DSGVO bzw. § 29 KDG-konformen Dienstleistungsvertrag gedacht und kann jedem Verantwortlichen (Auftraggeber) auf Anforderung zur Verfügung gestellt werden. Die getroffenen Maßnahmen unterliegen dem technischen Fortschritt und werden somit fortlaufend aktualisiert, wobei das bisher vorhandene Sicherheitsniveau nicht verringert wird.

Ergänzend sei noch erwähnt, dass es bei der opta data Finance GmbH IT-Notfallpläne, Datensicherungs-, Berechtigungs und Löschkonzepte sowie dokumentierte Prozessabläufe gibt.

Allgemeiner Teil

1. Name und Anschrift des Unternehmens:

opta data Finance GmbH
Berthold-Beitz-Boulevard 461
45141 Essen

2. Ansprechpartner mit Telefon, Fax und E-Mail:

Kundenmanagement
Katharina Hake
Tel.: 0201 3196-0
Fax: 0201 3196-222
E-Mail: service@optadata-gruppe.de

Internes Datenschutzmanagement
Marcel Schmick
Tel.: 0201 3196-204
Fax: 0201 3196-165
E-Mail: m.schmick@optadata-gruppe.de

Informationssicherheits-Beauftragter (ISB)
Matthias Langer
Tel.: 0201 3196-944
Fax: 0201 3196-165
E-Mail: m.langer@optadata-gruppe.de

3. Name der Verantwortlichen (Geschäftsführer):

Andreas Fischer
Mark Steinbach

4. Name und Kontaktdaten des Datenschutzbeauftragten:

Joachim Kramer
Datenschutz Kramer & Kramer GmbH
Büro für Datenschutz und Datensicherheit
Elsternweg 24
42555 Velbert
Tel.: 02052 92897-66
Fax: 02052 92897-67
E-Mail: j.kramer@datenschutz-kramer.de

5. Datenschutzbeauftragter:

5.1. Bestellung:

› externer Datenschutzbeauftragter gem. Art. 37 DSGVO

› Die schriftliche Bestellung vom 05.09.2009 liegt vor.

› Ehemals war Herr Günter Wolfgang Kramer, staatl. gepr. Betriebswirt EDV, externer Datenschutzbeauftragter (01.09.1987 – 04.09.2009).

5.2. 5.2. Qualifikation:

› Datenschutz-Auditor (TÜV), Zertifizierungsstelle für Personal TARZERT der TÜV Akademie Rheinland, Nr. 19553

› über 20 Jahre Erfahrung im IT-Bereich

› regelmäßige Fortbildungen

› Mitglied im Erfa-Kreis für Datenschutzbeauftragte der Region MEO

› GDD Mitglied

› Firma Datenschutz Kramer & Kramer GmbH mit über 30 Jahren Erfahrung im Datenschutz

6. Mitarbeiter der opta data Finance GmbH:

› Alle Mitarbeiter werden schriftlich zur Wahrung des Datengeheimnisses, der Schweigepflicht nach § 203 StGB und der Vertraulichkeit nach DSGVO, BDSG und SGB verpflichtet. Die Verpflichtung erfolgt auf einem seperaten Formular.

› Die der Verpflichtung zugrunde liegenden Gesetzestexte werden allen Mitarbeitern gegen Unterschrift ausgehändigt.

› Die Verpflichtung wird bei Einstellung durch das Personalbüro der opta data Finance GmbH vorgenommen.

› Von allen Mitarbeitern werden in sensiblen Bereichen werden polizeiliche Führungszeugnisse eingeholt.

› Alle Mitarbeiter werden regelmäßig durch den DSB zum Thema „Datenschutz und Datensicherheit" geschult.

› Eine Betriebsvereinbarung über die private Nutzung von E-Mail, Internet, Telefon und den Umgang mit Hard- und Software wird ausgehändigt.

› Darüber hinaus existieren Richtlinien zur Informationssicherheit und dem Datenschutz, die allen Mitarbeitern zentral zur Verfügung gestellt werden.

7. Verzeichnis der Verarbeitungstätigkeiten gem. Art. 30 DSGVO:

› Das „Verzeichnis der Verarbeitungstätigkeiten" liegt vor und ist Bestandteil eines Integrierten Managementsystems, in dem auch das Qualitäts-, Arbeitsschutz-, Risiko- und Notfallmanagement abgebildet werden.

Technische und organisatorische Maßnahmen:

1. Verwehrung des Zugangs für Unbefugte zu Verarbeitungsanlagen, mit denen die Verarbeitung durchgeführt wird (Zugangskontrolle):

› Closed-Shop-Betrieb

› Alle Gebäude werden per Video überwacht.

› Die Serverräume werden automatisch per Video überwacht, sobald sie betreten werden.

› Der Zutritt in die Produktionsräume ist nur per RFID möglich.

› Besucher müssen sich an den Zentralen anmelden.

› Besucher- und Mitarbeiterausweise authorisieren den Zutritt.

› Die Zentrale im Berthold-Beitz-Boulevard 461 ist rund um die Uhr, an 7 Tagen in der Woche besetzt.

› Der Wachdienst fährt außerhalb der Arbeitszeiten alle Standorte der Unternehmensgruppe in Essen regelmäßig an.

› Die Serverräume sind mit seperaten Sicherheitsschlössern bzw. Zahlencode-Schlössern ausgestattet.

› Es kann nachvollzogen werden, welche Tür wann und von wem geöffnet wurde (Logfiles in den Türzutrittssystemen).

2. Verhinderung des unbefugten Lesens, Kopierens, Veränderns oder Löschens von Datenträgern (Datenträgerkontrolle):

› Daten in Papierform werden gesammelt und in abschließbaren Containern entsorgt. Wenn die Container voll sind, werden sie von der Rhenus Data Office GmbH, Ratingen abgeholt und gemäß DIN 66399 datenschutzgerecht entsorgt (gegen Quittung).

› Elektronische und optische Datenträger werden in abgeschlossenen Alu-Tonnen in der IT-Abteilung in einem verschlossenen Raum gesammelt und von der Rhenus (Rhenus Data Office GmbH) vor Ort geschreddert.

› Magnetische Datenträger, wie Festplatten und LTO-Bänder, werden inventarisiert und der „Lebenszyklus" wird dokumentiert.

3. Verhinderung der unbefugten Eingabe von personenbezogenen Daten sowie der unbefugten Kenntnisnahme, Veränderung und Löschung von gespeicherten, personenbezogenen Daten (Speicherkontrolle) durch:

› Benutzername und Kennwort

› automatische Sperrung nach 5 Minuten Inaktivität (Pausenschaltung)

› Sperrung des Accounts bei wiederholter Falschanmeldung

› datenschutzgerechte Passwortrichtlinien gemäß BSI vom Domaincontroller vorgegeben oder vom Mitarbeiter bei der Erstanmeldung selbst generiert

› Active Directory mit Zugangsprotokoll

› Server mit zusätzlichen Administratorpasswörtern

› geschützte WLAN-Netzwerke/für Gäste separates WLAN und Speicherung in verschlüsselten Password-Depots

› Hardware in nicht öffentlichen Bereichen

› dokumentierte Prozesse bei der Benutzerverwaltung (DIN ISO 27001 und BaFin geprüft)

4. Verhinderung der Nutzung automatisierter Verarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung durch Unbefugte (Benutzerkontrolle) durch:

› G-Data-Virenscanner mit automatischem Update und automatischer Verteilung an die Clients

› Home-Office-Arbeitsplätze via VPN-Anbindung und Citrix Netscaler Terminalserver

› Patchmanagement der eingesetzten Software, Treiber und OS über Matrix42

› administrierte Firewalls (Cisco-Appliance aus Enterprise-Bereich)

› Server für externe Zugriffe in einer DMZ

5. Gewährleistung, dass die zur Benutzung eines automatisierten Verarbeitungssystems Berechtigten ausschließlich zu den von ihrer Zugangsberechtigung umfassten, personenbezogenen Daten Zugang haben (Zugriffskontrolle):

› Nur die jeweiligen Programmierer bzw. Systembetreuer haben Zugriff auf „ihr" System.

› Differenzierte Berechtigungen werden durch die Anmeldung gesteuert.

› Zusätzliche Administratorpasswörter für die Server sind nur den entsprechenden IT-Mitarbeitern bekannt und werden zusätzlich in einem verschlossenen Umschlag an einem separaten Ort sicher aufbewahrt.

› Zusatzvereinbarung für Systemadministratoren

6. **Gewährleistung, dass überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten mit Hilfe von Einrichtungen zur Datenübertragung übermittelt oder zur Verfügung gestellt wurden oder werden können (Übertragungskontrolle):**

   › Bei den Verbindungen werden VPN-Tunnelverbindungen genutzt.

   › Die Übertragung zu den Rechnungsprüfstellen der Kostenträger erfolgt mit Hilfe des Programms dacota und zertifizierter Schlüssel vom ITSG Trust Center (es wird ein asymmetrisches Kryptosystem mit Public-Private-Key benutzt).

   › Der Zugriff auf das Online Kundencenter ist nur nach dokumentierter Authentifizierung möglich.

7. **Gewährleistung, dass nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit und von wem in automatisierte Verarbeitungssysteme eingegeben oder verändert worden sind (Eingabekontrolle) durch:**

   › Protokolle am Domain-Controller

   › Server Protokolle

   › Protokollierung der Benutzerkennung im selbst erstellten Programmpaket eva/3 RZ bei jeder Datenveränderung

8. **Gewährleistung, dass bei der Übermittlung personenbezogener Daten sowie beim Transport von Datenträgern die Vertraulichkeit und Integrität der Daten geschützt werden (Transportkontrolle) durch:**

   › festgelegte Transportwege beim Versand von Daten in Papierform

   › Zugriff auf das Online Kundencenter nur über https-Protokoll

   › Scannen der ein- und ausgehende E-Mails vom Virenscanner

   › E-Mail -TLS-Verschlüsselung

9. **Gewährleistung, dass eingesetzte Systeme im Störungsfall wiederhergestellt werden können (Wiederherstellbarkeit) durch:**

   › Betrieb von redundanten Rechenzentren

   › Bearbeitung der Störung im Rahmen einer definierten Wiederherstellungsstrategie

   › Verfügung von Reserve-Server bei einem Ausfall

   › Aufbewahrung der LTO-Bänder in feuersicherem Tresor (DIS 120) in anderem Brandabschnitt

   › IT-Notfallpläne

10. **Gewährleistung, dass alle Funktionen des Systems zur Verfügung stehen und auftretende Fehlfunktionen gemeldet werden (Zuverlässigkeit) durch:**

    › Meldung von verschiedenen Systemfehlern (Plattenausfall, CPU-Ausfall, etc.) durch ein Monitoring-System

    › Meldung von Störungen durch Löschanlagen und Sauerstoffreduzierung

    › Umweltüberwachung in den Serverräumen

    › Serverräume mit Brand- und Rauchmelder, Alarmanlage, Klimaanlage und Videoüberwachung

    › IT-Infrastruktur mit Rufbereitschaft, auch außerhalb der Geschäftszeiten (24 Stunden , 7 Tage in der Woche besetzt)

11. **Gewährleistung, dass gespeicherte, personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden können (Datenintegrität) durch:**

    › Vermeidung der Datenhaltung auf lokalen Endgeräten

    › Patchmanagement nach DIN ISO 27001

12. **Gewährleistung, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Auftragskontrolle) durch:**

    › den Abrechnungsverträgen beiliegende Verträge zur Auftragsverarbeitung und Regelung der Kompetenzen und Pflichten zwischen Auftraggebern und der opta data Finance GmbH

    › dokumentierte Prozessabläufe

    › „Digitale Laufzettel", die von den einzelnen Mitarbeitern bei manuellen Tätigkeiten abgezeichnet werden, um zu sehen, welcher Mitarbeiter aus welcher Abteilung welchen Kunden bearbeitet hat (vom Posteingang über die Sortierung, Erfassung/Scan, Abrechnung, Buchhaltung und Versand).

    › interne Schulungen und Weiterbildungen

13. **Gewährleistung, dass personenbezogene Daten gegen Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle) durch:**

    › automatisiertes Backupverfahren mit Protokollen

    › hochverfügbares Storagecluster

    › vorhandene redundante Serverräume

    › Ausstattung aller Rechenzentren mit Raid-Systemen, die Daten permanent spiegeln

    › Anschluss aller Server an ausreichend dimensionierte USVs

    › Netzersatzanlage zur Überbrückung länger anhaltender Stromausfälle

    › Schutz des Serverraums vor Feuer durch Feuerschutztür und Stahlwände

    › gemäß Brandschutzklasse S30

14. **Gewährleistung, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden können (Trennbarkeit) durch:**

    › interne Mandantenfähigkeit

    › Installation verschiedener Systeme auf unterschiedlichen Servern

    › Trennung von Produktiv- und Testsystem

15. **Verfahren zur regelmäßigen Überprüfung und Bewertung der technischen und organisatorischen Maßnahmen im Datenschutz gem. Art. 32 Abs. 1 d) und Art. 25 Abs. 1 DSGVO**

    › Ein Datenschutzmanagement wurde eingeführt. Das Datenschutzmanagement-Team wird in die Planung neuer oder geänderter Projekte einbezogen und führt in regelmäßigen Abständen interne Audits durch.

    › Verantwortlichkeiten wurden festgelegt und technische und organisatorischen Maßnahmen werden regelmäßig evaluiert und aktualisiert.

    › eine Datenschutzleitlinie ist vorhanden

    › regelmäßige Schulungen der Mitarbeiter durch den Datenschutzbeauftragten

    › interne Audits werden regelmäßig durch das Datenschutzmanagement und das Qualitätsmanagement durchgeführt

    › Revision mit internen Audits

    Incident-Response-Management:

    › Es gibt Richtlinien, Handlungsanweisungen und Prozesse, die bei geänderten Voraussetzungen und bei Gesetzesänderungen angepasst werden. Ferner werden Prozesse immer wieder auf Funktionalität überprüft und ggf. angepasst oder erweitert.

    › Grafisch visualisierte Handlungsanweisungen für verschiedene Datenschutzprozesse wie z. B. Einbindung des DSB, Meldewege, Betroffenenrechte etc.

    › Datenschutzfolgeabschätzungen gem Art. 35 DSGVO werden für Prozesse bei denen besondere und sensible Daten verarbeitet werden durchgeführt.